1/19/1 **Links**
JAPIO

02951291 **Image available**
ENCIPHERMENT KEY DELIVERY SYSTEM

Pub. No.: 01-248891 [JP 1248891 A]
Published: October 04, 1989 (19891004)
Inventor: UMEMOTO AKITO
WATANABE HIROSHI
Applicant: KONDEISHIYONARU AKUSESU TECHNOL KENKYUSHO KK [000000] (A Japanese Company or Corporation), JP (Japan)
NEC CORP [000423] (A Japanese Company or Corporation), JP (Japan)
Application No.: 63-077296 [JP 8877296]
Filed: March 30, 1988 (19880330)
International Class: [4] H04N-007/167
JAPIO Class: 44.6 (COMMUNICATION -- Television)
Journal: Section: E, Section No. 867, Vol. 13, No. 594, Pg. 150, December 27, 1989 (19891227)

ABSTRACT
PURPOSE: To instantaneously deliver work keys to all receivers and to shorten the delivery time of the work keys at long cycles by composing inherent keys of common keys for the all receivers and different keys at every receiver, giving the work keys ciphered with the common keys for the receivers to the all receivers, and transmitting individual information other than the work key with enciphering by means of the different key at every receiver.

CONSTITUTION: In a ciphering device 103, common individual information KJ0 including a work key Kw is ciphered by a Km0, and converted into a signal eKJO. Individual information KJp different at every receiver is ciphered by a key KMp different at every receiver, and converted into a signal eKJp. On the other hand, on a receiving side, the transmitted signals eKJ0 and eKJp are decoded by the common key Km0 and the key Kmp different at every receiver in a decoder 106, and KJp and KJ0 are taken off. Further, the individual information KJp and program information BJ are compared by a comparator/collator 108. As a result, only when contract conditions correspond to watching permitting conditions, a switch 109 is conducted, and a scrambler key ks is outputted.

⑲日本国特許庁(JP)　⑪特許出願公開

⑫公開特許公報(A)　平1−248891

⑤1Int. Cl.⁴	識別記号	庁内整理番号	㊸公開　平成1年(1989)10月4日
H 04 N 7/167		8725−5C	

審査請求　有　請求項の数 1　(全4頁)

㊹発明の名称　暗号化鍵配送方式

㉑特　願　昭63−77296
㉒出　願　昭63(1988)3月30日

㉒発明者　梅本　明人　東京都港区虎ノ門1丁目20番7号
㉒発明者　渡辺　浩　東京都府中市日新町1−10　日本電気株式会社府中事業場内
㉑出願人　株式会社コンデイショナル・アクセス・テクノロジー研究所　東京都港区虎ノ門1丁目20番7号
㉑出願人　日本電気株式会社　東京都港区芝5丁目33番1号
㉔代理人　弁理士　浅村　皓　外3名

明細書の浄書(内容に変更なし)

明　細　書

1. 発明の名称

暗号化鍵配送方式

2. 特許請求の範囲

(1) 番組データにスクランブルをかけるためのスクランブル鍵と、このスクランブル鍵を含む番組情報を暗号化するワーク鍵と、このワーク鍵を含む個別情報を暗号化する固有鍵とによつて暗号化が行われ、暗号化された前記スクランブル鍵と前記ワーク鍵とを各受信者へ伝送する暗号化鍵配送方式において、

前記固有鍵は受信者共通の鍵と受信者ごとに異なる鍵とから成り、送信側において前記ワーク鍵は受信者共通の鍵によつて暗号化されると共にワーク鍵以外の前記個別情報は受信者ごとに異なる鍵によつて暗号化され、一方各受信者の側では前記固有鍵として前記の受信者共通の鍵と受信者ごとに異なる鍵を備え、前記個別情報を受信者共通の鍵によつて復号化することによりワーク鍵を抽出し、また前記個別情報を受信者ごとに異なる鍵によつて復号化することにより受信者の個別情報を抽出し、抽出された前記ワーク鍵で復号化された番組情報内の視聴許可条件と前記受信者の個別情報内の受信契約条件とが合致したとき前記ワーク鍵で抽出されたスクランブル鍵をデスクランブラに与えることを特徴とする暗号化鍵配送方式。

3. 発明の詳細な説明

[産業上の利用分野]

本発明は送信側で鍵によつてスクランブルされた放送番組データを受信側でデスクランブルするための暗号化鍵配送方式に関する。

[従来の技術]

第2図は従来のスクランブル用暗号化鍵の配送方式を示している。第2図中、左側は送信側を示し、右側は受信側を示している。

送信側において暗号化のための鍵はスクランブル鍵KsとワークKwと固有鍵Kmpの3種類の鍵が存在する。番組データBDは、受信者共通の放送番組データであり、スクランブラ101においてスクランブル鍵Ksでスクランブルされ信

号ｅＢＤに変換される。ＢＪは受信者共通の番組に付随した番組情報であり、この番組情報ＢＪは視聴許可条件（例えば番組価格、視聴条件のコード等）とスクランブル鍵Ｋｓ等で構成される。番組情報ＢＪは暗号器１０２においてワーク鍵Ｋｗによつて暗号化され信号ｅＢＪに変換される。上記スクランブル鍵Ｋｓは通常約１秒位で更新される短周期の鍵である。また、個別情報（ＫＪ）群の中のＫＪｐは、特定の受信者ｐ（例えばｐさん）固有の個別情報であり、この個別情報ＫＪｐは、契約条件（支払い金額、有効日数、視聴条件のコード等）とワーク鍵Ｋｗ等で構成され、暗号器１０３において受信者ｐの固有鍵Ｋｍｐで暗号化され信号ｅＫＪｐに変換される。上記ワーク鍵Ｋｗは通常約１カ月位で更新される長周期の鍵である。第２図中個別情報（ＫＪ）群はＫＪ１，ＫＪ２，……ＫＪｎで構成され（ｎは受信者数）、ＫＪｐはＫＪ群のいずれか一つを表わす。ＫＪ群のすべてはそれぞれ暗号器１０３で固有鍵（Ｋｍ）群の対応する固有鍵で暗号化されｅＫＪ群となる。受信者固有の鍵群は、各受信者が１個ずつ保有している鍵Ｋｍ１，Ｋｍ２，……，Ｋｍｐ，……，Ｋｍｎで構成される。

上記の信号ｅＢＤ，ｅＢＪの多数のｅＫＪは、合成器１０４で合成された後、各受信者宛に配送される。

一方、受信側においては、各受信者宛に配送された信号ｅＢＤ，ｅＢＪと多数のｅＫＪは、分離器１０５で選択分離され、信号ｅＢＤ，ｅＢＪ及び自分宛の情報ｅＫＪｐのみを抽出する。最初にｅＫＪｐが復号器１０６で受信者ｐの固有鍵ｋｍｐで元のＫＪｐに復号化される。次にｅＢＪが、復号器１０７において、ＫＪｐの中に含まれる受信者共通のワーク鍵Ｋｗを用いて元のＢＪに復号化される。最後に、前記ＫＪに含まれた契約条件とＢＪに含まれた視聴許可条件とが比較照合器１０８において一致すると判定された場合にのみ切替器１０９が導通状態になり、デスクランブラ１１０においてｅＢＤがＢＪの中に含まれるスクランブル鍵によつてデスクランブルされる。このようにして受信者側にて元の番組データＢＤが取り出され、視聴される。

［発明が解決しようとする問題点］

前述した従来の鍵配送方式では、例えば受信者が１０００万人であるとすると、仮に１つの伝送路でのワーク鍵Ｋｗの配送能力が１時間に１００万人であつたとしても、ワーク鍵を各受信者の固有鍵で暗号化して各受信者ごとに個別に配送しているので、すべての受信者にワーク鍵Ｋｗを配送するには最低でも１０時間を必要とする。また、受信者が常時受信待機をすることができない場合や伝送路で生じるエラーを考慮してワーク鍵を数回送出する場合にはワーク鍵Ｋｗの配送時間として数十時間以上の時間が必要となる。このように従来の鍵配送方式では、受信者が多数の場合ワーク鍵を送出するための時間が問題となり、一伝送路だけではワーク鍵Ｋｗをすべての受信者に短時間で配送することができないという欠点を有している。

本発明の目的は、受信者が多数であつてもワーク鍵Ｋｗを短時間で配送することのできる暗号化鍵配送方式を提供することにある。

［問題点を解決するための手段］

本発明に係る暗号化鍵配送方式は、受信側では個別情報の契約条件と番組情報の視聴許可条件とが一致するという条件の下でスクランブル鍵が取り出されることを考慮して、固有鍵を受信者共通の鍵と受信者ごと異なる鍵で構成し、ワーク鍵を受信者共通の鍵で暗号化して受信者全員に与えることとし、ワーク鍵以外の個別情報は受信者ごと異なる鍵で暗号化し伝送するように構成される。

［実施例］

以下に本発明の実施例を添付図面に従つて説明する。

第１図は本発明に係る暗号化鍵配送方式を示すブロック図であり、第１図中左側に送信側装置を、右側に受信側装置を示す。第１図において、基本的構成は第２図で示した従来のものと同じであるので、第１図中第２図で示した同一要素には同一符号を付し、その詳細な説明を省略する。すなわ

ち、１０１は番組データＢＤをスクランブルするスクランブラ、１０２は番組情報ＢＪを暗号化する暗号器、１０３は個別情報を暗号化する暗号器、１０４は合成器、１０５は分離器、１０６は個別情報を復号する復号器、１０７は番組情報を復号する復号器、１０８は比較照合器、１０９は切替器、１１０はデスクランブラである。上記の各構成要素の機能は従来技術の箇所で説明した通りである。

次に本発明の特徴的部分を説明する。送信側の固有鍵（Ｋｍ）群には、各受信者ごとに異ならせた固有鍵Ｋｍ１，Ｋｍ２，……Ｋｍｐ，……Ｋｍｎと受信者のすべてに共通する鍵Ｋｍ０とが含まれる。上記においてｎは整数で受信者の数を表わし、ｐは任意の受信者を表わす符号である。暗号器１０３は個別情報（ＫＪ）群の中に含まれる個別情報ＫＪｐの暗号化を行うが、この場合にはワーク鍵Ｋｗを含む共通の個別情報ＫＪ０とそれ以外の個別情報ＫＪｐとを別々に暗号化する。すなわち、暗号器１０３においてワーク鍵Ｋｗを含む共通の個別情報ＫＪ０は鍵Ｋｍ０で暗号化されて信号ｅＫＪ０に変換され、他の受診者ごとに異なる個別情報ＫＪｐは受信者ごとに異なる鍵Ｋｍｐによつて暗号化され信号ｅＫＪｐに変換される。

一方、受信側においては、復号器１０６で、伝送されてきた上記信号ｅＫＪ０とｅＫＪｐとを、各受信者に設けられた共通の鍵Ｋｍ０と受信者ごとに異なる鍵Ｋｍｐとでそれぞれ復号化し、ＫＪｐとＫＪ０を取り出す。そして個別情報ＫＪ０のワーク鍵Ｋｗを用いて復号器１０７で番組情報ＢＪを取り出し、比較照合器１０８で個別情報ＫＪｐと番組情報ＢＪを比較し、契約条件と視聴許可条件が一致したときにのみ切替器１０９を導通させ、スクランブラ鍵Ｋｓを出力させる。

上記の実施例において、受信者に共通の鍵Ｋｍ０は全受信者に対して共通としたが、全受信者を複数のブロックに分け、ブロックごとに異なる鍵を設け、複数の鍵として構成できる。このように必要に応じて受信者に共通な鍵を数個以上使用することもできる。

［発明の効果］

以上の説明で明らかなように本発明によれば、固有鍵の中に受信者に共通な鍵を用意し、この鍵でワーク鍵を暗号化するようにしたため、ワーク鍵を瞬時に全受信者に配送でき、長周期のワーク鍵の配送時間を大幅に短縮できる。また、受信者が１カ月単位の短期契約であつても、必要な時期に随時ワーク鍵を変更できるという効果も発揮される。

4．図面の簡単な説明

第１図は本発明に係る暗号化鍵配送方式を説明するためのブロック図、

第２図は従来の暗号化鍵配送方式を説明するためのブロック図である。

［符号の説明］

１０１……スクランブラ

１０２，１０３……暗号器

１０４……合成器

１０５……分離器

１０６，１０７……復号器

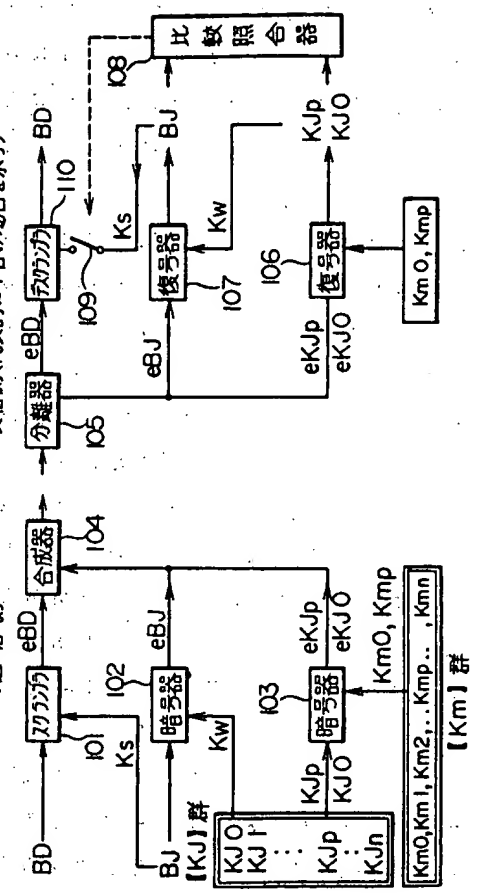
１０８……比較照合器

１１０……デスクランブラ

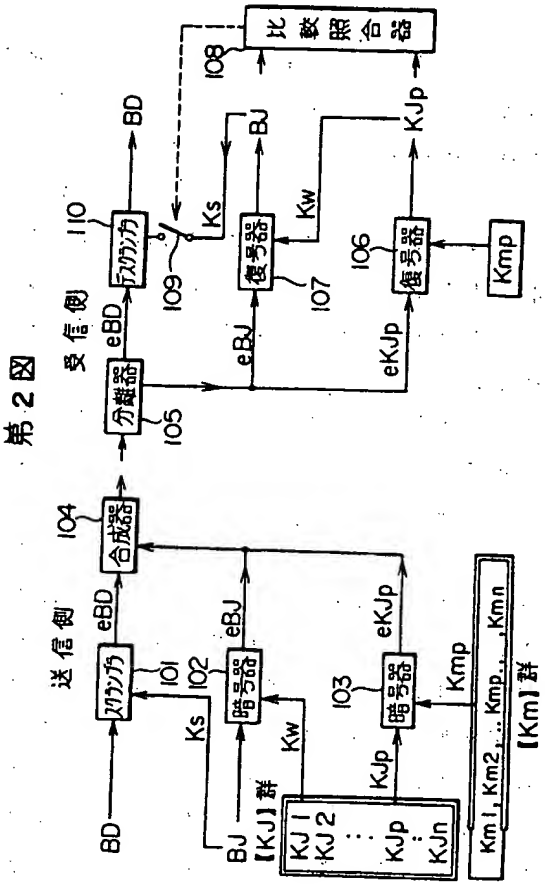
代理人　浅　村　　皓

図面の浄書（内容に変更なし）

第1図



第2図



手　続　補　正　書（方式）

特許庁長官殿　　昭和 63 年 7 月 28 日

1．事件の表示

昭和 63 年　特許願第 077296 号

2．発明の名称

暗号化履歴送信方式

3．補正をする者

事件との関係　特許出願人
氏名（名称）

株式会社 コンディショナル・アクセス・テクノロジー研究所

4．代　理　人　（ほか 1 名）

居　所　〒100 東京都千代田区大手町二丁目2番1号
新大手町ビルヂング 331
電　話（211）3851（代表）
氏　名　（6669）弁理士 澤 村 純

5．補正命令の日付　昭和 63 年 6 月 28 日

6．補正により増加する請求項の数

7．補正の対象

代理権を証明する書面（日本電気株式会社の分）
明細書
図面

特許庁 63. 7. 28 出願第二課

8．補正の内容　別紙のとおり　方式審査

願書に最初に添付した明細書の浄書（内容に変更なし）
願書に最初に添付した図面の浄書（内容に変更なし）